



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/641,312	08/18/2000	Ryuji Ishiguro	SONY-T0988	7225
22850	7590	01/04/2005		
OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C. 1940 DUKE STREET ALEXANDRIA, VA 22314			EXAMINER MOORTHY, ARAVIND K	
			ART UNIT 2131	PAPER NUMBER

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/641,312

Applicant(s)

ISHIGURO ET AL.

Examiner

Aravind K Moorthy

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 July 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 19 July 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1-25 are pending in the application.
2. Claims 1-25 have been rejected.

Response to Amendment

3. The examiner approves the amendments made to figures 5 and 7A.

Response to Arguments

4. Applicant's arguments with respect to claims 1-11 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Art Unit: 2131

5. Claims 6-11 are rejected under 35 U.S.C. 102(e) as being anticipated by Aucsmith et al U.S. Patent No. 5,940,513.

As to claims 6, 9 and 10, Aucsmith et al discloses a receiver device for receiving first data from a transmitter device, the receiver device comprising:

communication means which, in the authenticating of the transmitter device, receives, from the transmitter device, second data that describes a limitation on the usage of the first data while transmitting check value calculated on the basis of the second data to the transmitter device [column 4, lines 47-61];
and

encrypted value generator means for generating the check value of the second data based on the second data received by the communication means, in the authenticating of the transmitter device, the check value for detecting whether the second data has been tampered with or not [column 5, lines 62-67].

As to claim 7, Aucsmith et al discloses a receiver device further comprising a random number generator means for generating a random number having a predetermined bit number [column 5, lines 36-61]. Aucsmith et al discloses that the communication means transmits, to the transmitter device, the check value of the second data together with the random number generated by the random number generator means [column 5, lines 36-61].

As to claim 8, Aucsmith et al discloses a receiver device further comprising a usage limiting data generator means which generates, subsequent to the reception of the first data, third data which describes a limitation on the usage of the first data, based on the second data received by the communication means [column 7, lines 31-51]. Aucsmith et al discloses that the

Art Unit: 2131

encrypted value generator means generates a check value generated on the basis of the third data generated by the usage limiting data generator means [column 7, lines 14-30]. Aucsmith et al discloses that the communication means transmits, to the transmitter device, the check value of the second data together with the check value of the third data [column 8, lines 43-59].

As to claim 11, Aucsmith et al discloses a communication system comprising a transmitter device which transmits first data by driving a recording medium that stores the first data and second data that describes a limitation on the usage of the first data, and a receiver device for receiving the first data;

the transmitter device comprising:

storage means for storing a check value calculated on the basis of the second data [column 7, lines 1-13];

first communication means which, in the authenticating of the receiver device, transmits the second data to the receiver device while receiving a check value calculated on the basis of the second data from the receiver device [column 7, lines 14-30]; and

determination means which, in the authenticating of the receiver device, determines whether the check value of the second data received by the communication means matches the check value of the second data stored in the storage means [column 7, lines 14-30]; and

the receiver device comprising:

second communication means which, in the authenticating of the transmitter device [column 4 line 62 to column 5 line 9],

receives, from the transmitter device, second data that describes a limitation on the usage of the first data while transmitting the check value calculated on the basis of the second data to the transmitter device [column 4 line 62 to column 5 line 9]; and

encrypted value generator means for generating the check value of the second data based on the second data received by the communication means, in the authenticating of the transmitter device, the check value for detecting whether the second data has been tapered with or not [column 5, lines 25-67].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1, 2, 4 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Epstein U.S. Patent No. 6,490,355 B1 in view of Balcha et al U.S. Patent No. 6,233,589 B1.

As to claims 1, 4 and 5, Epstein discloses a transmitter device which transmits first data to a receiver device by driving a recording medium that stores the first data and second data that describes a limitation on the usage of the first data, the transmitter device comprising:

storage means for storing a check value of calculated on the basis of the second data [column 7, lines 55 to column 8 line 7];

communication means which, in the authenticating of the receiver device, transmits the second data to the receiver device while receiving a check value

calculated on the basis of the second data from the receiver device [column 8, lines 10-24]; and

determination means which, in the authenticating of the receiver device, determines whether check value of the second data received by the communication means matches the check value of the second data stored in the storage means [column 8, lines 25-51].

Epstein does not teach that the check value is used to detect whether the second data is tampered with or not.

Balcha et al teaches a hashing function that is used to detect whether the second data is tampered with or not [column 10, lines 23-29].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Epstein so that the hashing functions would have also been used to detect whether the second data is tampered with or not.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Epstein by the teaching of Balcha et al because the hash is cumulative and it is possible to detect when both a block of data and the corresponding hash have been replaced on the storage medium when the replacement hash and all following hashes are not determined using the specific cumulative hash function used during the original writing of the data. Further, if there is an accidental error, attempts to recover the lost data can be made and the cumulative hash can be used to verify the recovered data [column 4, lines 1-16].

Art Unit: 2131

As to claim 2, Epstein teaches that the storage means inhibits the writing or reading of the check value of the second data in a process other than the authentication process [column 9 line 53 to column 10 line 10].

7. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Epstein U.S. Patent No. 6,490,355 B1 and Balcha et al U.S. Patent No. 6,233,589 B1 as applied to claim 1 above, and further in view of Bernecker U.S. Patent No. 5,435,599.

As to claim 3, the Epstein-Balcha combination does not teach that the storage means has a tamper resistance.

Bernecker teaches a tamper resistant storage medium and its benefits [abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Epstein-Balcha combination so that the storage medium as taught in the combination above would have been tamper resistant.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Epstein-Balcha combination by the teaching of Bernecker because it solves the problem of falsification and tampering of recording mediums [column 2 line 67 to column 3 line 15]

8. Claims 12-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Linnartz U.S. Patent No. 6,209,092 B1 in view of Balcha et al U.S. Patent No. 6,233,589 B1.

As to claims 12 and 17, Linnartz discloses a transmitter device for transmitting a content to a receiver device comprising:

a memory configured to store a hash value of a content management data
in relation to the content [column 4 line 58 to column 5 line 2];

communicating means for transmitting the content management data of the content and receiving a hash value calculated at the receiver device on the basis of the content management data from the receiver device [column 5, lines 3-26];

comparing means for comparing the check value in the storage and the check value transmitted from the receiver device [column 6, lines 23-45]; and

Linnartz does not teach determining means for determining whether the content management data is tempered or not, on a basis of a result provided by the comparing means.

Balcha et al teaches a hashing function that is used to detect whether the second data is tampered with or not [column 10, lines 23-29].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Linnartz so that the hashing functions would have also been used to detect whether the second data is tampered with or not.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Linnartz by the teaching of Balcha et al because the hash is cumulative and it is possible to detect when both a block of data and the corresponding hash have been replaced on the storage medium when the replacement hash and all following hashes are not determined using the specific cumulative hash function used during the original writing of the data. Further, if there is an accidental error, attempts to recover the lost data can be made and the cumulative hash can be used to verify the recovered data [column 4, lines 1-16].

As to claim 13, Linnartz teaches that the content management data is changed when the content is used and the status of the content is changed [column 7 line 27 to column 8 line 10].

Art Unit: 2131

As to claim 14, Linnartz teaches that the management data is changed when the content is used and the status of the content is changed [column 7 line 27 to column 8 line 10].

As to claim 15, Linnartz teaches that the content management data is in accordance with at least one of a reproduction of the content, a copying of the content, and a movement of the content [column 7 line 27 to column 8 line 10].

As to claim 16, Linnartz teaches that the content management data is at least one of a number of the reproduction of the content and a number of the copying of the content [column 7 line 27 to column 8 line 10].

As to claims 18 and 23-25, Linnartz discloses a computer implemented program that when executed by a processor implements steps comprising:

storing a check value of a content management data in relation to the content [column 4 line 58 to column 5 line 2];

transmitting the content management data of the content and receiving a check value calculated at a receiver on the basis of the content management data from the receiver [column 5, lines 3-26];

comparing the check value stored in the storing step with the check value transmitted from the receiver [column 6, lines 23-45]; and

Linnartz does not teach determining whether the content management data has been tampered with or not, on a basis of a result by the comparing step.

Balcha et al teaches a hashing function that is used to detect whether the second data is tampered with or not [column 10, lines 23-29].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Linnartz so that the hashing functions would have also been used to detect whether the second data is tampered with or not.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Linnartz by the teaching of Balcha et al because the hash is cumulative and it is possible to detect when both a block of data and the corresponding hash have been replaced on the storage medium when the replacement hash and all following hashes are not determined using the specific cumulative hash function used during the original writing of the data. Further, if there is an accidental error, attempts to recover the lost data can be made and the cumulative hash can be used to verify the recovered data [column 4, lines 1-16].

As to claim 19, Linnartz teaches that the content management data indicates an authorized usage of the content data [column 7 line 27 to column 8 line 10].

As to claim 20, Linnartz teaches that the content management data is changed when the content is used and a status of the content is changed [column 7 line 27 to column 8 line 10].

As to claim 21, Linnartz teaches that the content management data is in accordance with at least one of a reproduction of the content, a copying of the content, and a movement of the content [column 7 line 27 to column 8 line 10].

As to claim 22, Linnartz teaches that the content management data is at least one of a number of the reproductions of the content and a number of copies of the content [column 7 line 27 to column 8 line 10].

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

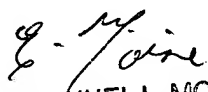
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
December 20, 2004


EMMANUELL L. MOISE
PRIMARY EXAMINER